AFRL-OSR-VA-TR-2015-0151

(YIP-10) NEW MODELS FOR PROTOCOL SECURITY

Rafael Pass
CORNELL UNIVERSITY

07/06/2015
Final Report

DISTRIBUTION A: Distribution approved for public release.

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTC
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
18-06-2015

2. REPORT TYPE
Final Report

3. DATES COVERED *(From - To)*
01-04-2010 - 31-03-2015

4. TITLE AND SUBTITLE
AFOSR: YIP: New Models for Protocol Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-10-1-0093

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Rafael Pass
Department of Computer Science
Cornell NYC Tech
New York, NY 10011

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Cornell University
111 Eighth Avenue #302
New York, NY 10011

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Office of Scientific Research
875 Randolph Street
Suite 325 Room 3112
Arlington , VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A - Approved for Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Following the ground-breaking work on public-key encryption in the 70's, the field of Cryptography has evolved far beyond securing message transmission. This novel use of cryptography, however, also admits new types of attacks, which require studying new models of security. During the reporting period, we have focused on two major directions within this topic: security under concurrent executions, and security under tampering attacks.
Our research has been published in the premier Computer Science Theory conferences (STOC, FOCS, ITCS), and the premier Cryptography conferences (CRYPTO, EuroCrypt, TCC); 5 of these papers were selected for special issues on best papers.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					19b. TELEPHONE NUMBER *(Include area code)*

Reset

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

New Models for Protocol Security: AFOSR YIP Award FA9550-10-1-0093 4/1/2010-3/31/2015 **Final Report**

Rafael Pass
Department of Computer Science
Cornell NYC Tech
New York, NY 10011

1 Introduction

Following the ground-breaking work on public-key encryption in the 70's, the field of Cryptography has evolved far beyond securing message transmission. Today, cryptographic protocols are used in large-scale systems to guarantee not only confidentiality and authenticity but also attack- and fault-tolerance.

For instance, the notion of a *secure computation*, introduced by Yao and Goldreich, Micali and Wigderson in the early 80's, enables a set of parties to, through the execution of a distributed communication protocol, securely implement any service that a trusted party could perform for them. More precisely, a secure computation protocol allows n mutually distrustful parties, each with their individual private input, to evaluate any (efficiently computable) function of their respective inputs, while maintaining the same security as if a trusted third party had performed the computation. Security here means that, even if an arbitrary subset of the parties get corrupted and deviate from their prescribed instructions, both correctness and confidentiality is still maintained.

Another central notion is that of a *zero-knowledge proofs*. Zero-knowledge proofs (introduced Goldwasser, Micali and Rackoff) are protocols that enable one party—called the *prover*—to convince another party—called the *verifier*—about the validity of some mathematical statement without revealing anything else about the content of the statement. Zero-knowledge protocols are often used as authentication protocols: I can convince you that I know the secret key associated with a particular public key but without actually revealing the secret key.

This novel use of cryptography, however, also admits new types of attacks, which require studying *new models of security*. During the reporting period, we have focused on two major directions within this topic: *security under concurrent executions*, and *security under tampering attacks*.

Below we discuss some of our major acheivments on these topics. Our research has been published in the most prestigious Computer Science Theory conferences (STOC, FOCS, ITCS), and the most prestigious Cryptography conferences (CRYPTO, EuroCrypt, TCC); 5 of these papers were selected for special issues on best papers.

2 Concurrent Security

The security of most cryptographic protocols (and, in particular, those for secure computation) can be compromised if many instances of the protocol are *concurrently* executed. This concurrent setting allows a coordinated attack in which an adversary controls many parties, interleaving the executions of the various protocol instances. For instance, a so called *man-in-the-middle* attacker participating in two simultaneous executions of a cryptographic protocol might use messages from one of the executions in order to violate the security of the second.

Consider a two-party protocol between A acting as an *initiator*, and B acting as a *responder*. A man-in-the-middle adversary M controlling the channel between A and B can participate in an interaction with A, acting as a responder, and at the same time participate in an interaction with B, acting as an initiator. Furthermore, by exploiting the interaction with A, M might be able to violate the security of the interaction with B. At a first glance, it seems that such an attack can be prevented by encrypting all communication between A and B. This does not work: If M is acting as truthful responder in its interaction with A, then A will believe that M is the rightful owner of the messages she sends, and thus encrypt all her messages using M's key. The same holds for B. Indeed Lowe's famous attack on the Needham-Schroeder protocol works this way.

On the Internet concurrent attacks are unavoidable. While both the need and definitions were articulated in the early 90's, constructions of concurrently secure protocols were lacking.

During the reporting period, we have developed several novel techniques for dealing with concurrent attacks, leading to the resolution of several decade-old open problems:

- We obtained the first *constant-round* construction for defending against man-in-the-middle attacks based the minimal assumption of one-way functions; this had remained a major open problem for over 20 years. Our paper was just accepted for publication in the *Journal of the ACM* (the most prestigous journal in Computer Science).
- We obtained the first *constant-round* secure computation protocols based on *minimal hardness assumptions*, resolving a central problem open since the conception of secure multi-party computation in 1987.
- We constructed the first secure computation protocols that require no trusted infrastructure other than authenticated communication, and that satisfy a meaningful notion of security that is preserved under concurrent executions assuming standard cryptographic hardness assumptions.
- We demonstrated the first construction of concurrently secure protocols that only use underlying cryptographic primitives as a *black-box*, demonstrating that practical solution may be within reach.
- We demonstrated the first *constant-round* concurrently secure protocol for the specific class of zero-knowledge protocols, based on reasonable hardness assumptions. This had remained an open problem since the original work by Dwork, Naor and Sahai from 1999.

3 Security in the Presence of Physical Attacks

The traditional definition of security assumes that honest players internal states are completely hidden from the attacker, and the only way for the attacker to learn something about, or affect, the internal state is by proving *inputs* and receiving *outputs* from honest parties. This is an unrealistic assumption that has been proven wrong in many setting.

During this reporting period, we have focused on analyzing the security of cryptographic protocols in the presence of stronger attacker that may access honest parties in more realistic ways. In particular, we have considered security in the context of *tampering* attackers, that may tamper with the internal state of honest parties.

- *Resettable security:* A very natural type of tamperings considers security of primitives in the presence of an attackers that may "reset" and "restart" an honest party, forcing them to return to an earlier state of the computation, and reusing the same random tape. This model is particularly relevant for cryptographic protocols being executed on embedded devices, such as smart cards. Since these devices have neither a built-in power supply, nor a non-volatile re-writable memory, they can be "reset" by simply disconnecting and reconnecting the power supply.) This notion of security is referred to as resettable security and its study was initiated in 2000. While constructions of resettable-secure protocols have been extensively since their conception, all these constructions relied on stronger than typical cryptographic hardness assumptions. In a sequence of works appearing in STOC 2013, FOCS 2013 (2 on this topic), and TCC 2014, we resolved some of central outstanding open questions in this field—namely, we showed construction under *minimal hardness* assumptions, and using a minimal number of *communication rounds*.
- *Tamper-resilient Security:* We initiate a study of the security of cryptographic primitives in the presence of efficient tampering attacks to the randomness of honest parties. More precisely, we consider p-tampering attackers that may tamper with each bit of the honest parties' random tape with probability p, but have to do so in an "online" fashion. We present both positive and negative results:
  - Any secure encryption scheme, bit commitment scheme, or zero-knowledge protocol (these are some of the most important cryptographic building blocks) can be broken with probability p by a p-tampering attacker. The core of this result is a new Fourier analytic technique for biasing the output of bounded-value functions, which may be of independent interest.
  - Assuming the existence of one-way functions, cryptographic primitives such as signatures, identification protocols can be made resilient to p-tampering attacks for any $p = 1/n^{\alpha}$, where $\alpha > 0$ and n is the security parameter.

4 Other Significant Results

Limits of Provable Security Modern Cryptography relies on the principle that cryptographic schemes are proven secure based on mathematically precise assumptions; these can be general—such as the existence of one-way functions—or specific—such as the hardness of factoring products of large primes. The security proof is a reduction that transforms any attacker A of the scheme into a machine that breaks the underlying assumption (e.g., inverts an alleged one-way function). During the past four decades, many cryptographic tasks have been based on a number of well-studied complexity-theoretic intractability assumptions. But there are some well-known protocols and primitives (e.g., Schnorrs identification scheme, commitment schemes secure against selective openings, Chaum Blind Signatures, etc.) that have resisted security reductions under well-studied intractability assumptions. What makes these protocols and primitives intriguing is that no attacks on them are known (and some of them are actually in use on the Internet). In a work from STOC'11, I demonstrate that for many of these primitives/protocols (and in particular, the above-mentioned ones), if their security can be based on any standard assumption using a Turing security reduction, then the assumption can be broken in polynomial time. In a line of subsequent works, we have extended this framework to deal with more primitives and stronger proof techniques.

Techniques for Program Obfuscation The goal of program obfuscation is to "scramble" a computer program, hiding its implementation details while preserving functionality. Unfortunately, the "dream" notion of security, guaranteeing that obfuscated code does not reveal any information beyond black-box access to the original program, has run into strong impossibility results, and is known to be unachievable for general programs Recently, the first plausible candidate for general-purpose obfuscation was presented by Garg et al for a relaxed notion of security, referred to as indistinguishability obfuscation (iO). During the past year, we have been been working on developing a sound foundation for program obfuscation. (This general topic will be further explored in our follow-up grant "Foundations and Applications of Program Obfuscation".)

In a recent work appearing in CRYPTO'14 we presented a new hardness assumption—the existence of "semantically secure multilinear encodings"—which generalizes a multilinear DDH assumption and demonstrate the existence of indistinguishability obfuscation for all polynomial-size circuits under this assumption (and the most standard "LWE assumption"). This work is the first to demonstrate that security reductions can be used to reduce obfuscation to some general intractability assumption (rather than just assuming that the construction is secure). (After our work, several other assumptions have been introduced by the research community.)

5 Publications During Reporting Period

1. Huijia Lin, Rafael Pass: Constant-Round Nonmalleable Commitments from Any One-Way Function. J. ACM 62(1): 5:1-5:30 (2015)

2. Joseph Y. Halpern, Rafael Pass: Algorithmic rationality: Game theory with costly computation. J. Economic Theory 156: 246-268 (2015)

3. Samantha Leung, Edward Lui, Rafael Pass: Voting with Coarse Beliefs. ITCS 2015: 61
4. Jing Chen, Silvio Micali, Rafael Pass: Better Outcomes from More Rationality. ITCS 2015: 325
5. Kai-Min Chung, Edward Lui, Rafael Pass: From Weak to Strong Zero-Knowledge and Applications. TCC (1) 2015: 66-92
6. Kai-Min Chung, Rafael Pass: Tight Parallel Repetition Theorems for Public-Coin Arguments Using KL-Divergence. TCC (2) 2015: 229-246
7. Vipul Goyal, Huijia Lin, Omkant Pandey, Rafael Pass, Amit Sahai: Round-Efficient Concurrently Composable Secure Computation via a Robust Extraction Lemma. TCC (1) 2015: 260-289
8. Edward Lui, Rafael Pass: Outlier Privacy. TCC (2) 2015: 277-305
9. Rafael Pass, Wei-Lung Dustin Tseng, Muthuramakrishnan Venkitasubramaniam: Concurrent Zero Knowledge, Revisited. J. Cryptology 27(1): 45-66 (2014)
10. Kai-Min Chung, Zhenming Liu, Rafael Pass: Statistically-secure ORAM with (log2 n) Overhead. ASIACRYPT (2) 2014: 62-81
11. Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, Karn Seth: On the Impossibility of Cryptography with Tamperable Randomness. CRYPTO (1) 2014: 462-479
12. Rafael Pass, Karn Seth, Sidharth Telang: Indistinguishability Obfuscation from Semantically-Secure Multilinear Encodings. CRYPTO (1) 2014: 500-517
13. Ilan Komargodski, Tal Moran, Moni Naor, Rafael Pass, Alon Rosen, Eylon Yogev: One-Way Functions and (Im)Perfect Obfuscation. FOCS 2014: 374-383
14. Joseph Y. Halpern, Rafael Pass, Lior Seeman: The truth behind the myth of the folk theorem. ITCS 2014: 543-554
15. Adam Bjorndahl, Joseph Y. Halpern, Rafael Pass: Axiomatizing Rationality. KR 2014
16. Rafael Pass, Karn Seth: On the Impossibility of Black-Box Transformations in Mechanism Design. SAGT 2014: 279-290
17. Elette Boyle, Kai-Min Chung, Rafael Pass: On Extractability Obfuscation. TCC 2014: 52-73
18. Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, Ivan Visconti: 4-Round Resettably-Sound Zero Knowledge. TCC 2014: 192-216
19. Joseph Y. Halpern, Rafael Pass, Lior Seeman: Not Just an Empty Threat: Subgame-Perfect Equilibrium in Repeated Games Played by Computationally Bounded Players. WINE 2014: 249-262

20. Joseph Y. Halpern, Rafael Pass: Conservative belief and rationality. Games and Economic Behavior 80: 186-192 (2013)

21. Rafael Pass, Alon Rosen, Wei-Lung Dustin Tseng: Public-Coin Parallel Zero-Knowledge for NP. J. Cryptology 26(1): 1-10 (2013)

22. Kai-Min Chung, Rafael Pass: Guest column: parallel repetition theorems for interactive arguments. SIGACT News 44(1): 50-69 (2013)

23. Kai-Min Chung, Huijia Lin, Rafael Pass: Constant-Round Concurrent Zero Knowledge from P-Certificates. FOCS 2013: 50-59

24. Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Ivan Visconti: Simultaneous Resettability from One-Way Functions. FOCS 2013: 60-69

25. Ran Canetti, Huijia Lin, Rafael Pass: From Unprovability to Environmentally Friendly Protocols. FOCS 2013: 70-79

26. Kai-Min Chung, Rafael Pass, Sidharth Telang: Knowledge-Preserving Interactive Coding. FOCS 2013: 449-458

27. Adam Bjorndahl, Joseph Y. Halpern, Rafael Pass: Language-Based Games. IJCAI 2013

28. Joseph Y. Halpern, Rafael Pass: Sequential Equilibrium in Computational Games. IJCAI 2013

29. Kai-Min Chung, Edward Lui, Rafael Pass: Can theories be tested?: a cryptographic treatment of forecast testing. ITCS 2013: 47-56

30. Per Austrin, Johan Hstad, Rafael Pass: On the power of many one-bit provers. ITCS 2013: 215-220

31. Kai-Min Chung, Huijia Lin, Mohammad Mahmoody, Rafael Pass: On the power of nonuniformity in proofs of security. ITCS 2013: 389-400

32. Kai-Min Chung, Rafael Pass, Karn Seth: Non-black-box simulation from one-way functions and applications to resettable security. STOC 2013: 231-240

33. Rafael Pass: Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments. TCC 2013: 334-354

34. Eleanor Birrell, Kai-Min Chung, Rafael Pass, Sidharth Telang: Randomness-Dependent Message Security. TCC 2013: 700-720

35. Joseph Y. Halpern, Rafael Pass: Iterated regret minimization: A new solution concept. Games and Economic Behavior 74(1): 184-207 (2012)

36. Tom Roeder, Rafael Pass, Fred B. Schneider: Multi-Verifier Signatures. J. Cryptology 25(2): 310-348 (2012)

37. Rafael Pass, Muthuramakrishnan Venkitasubramaniam: A Parallel Repetition Theorem for Constant-Round Arthur-Merlin Proofs. TOCT 4(4): 10 (2012)

38. Joseph Y. Halpern, Rafael Pass, Lior Seeman: I'm Doing as Well as I Can: Modeling People as Rational Finite Automata. AAAI 2012

39. Rafael Pass, Huijia Lin, Muthuramakrishnan Venkitasubramaniam: A Unified Framework for UC from Only OT. ASIACRYPT 2012: 699-717

40. Huijia Lin, Rafael Pass: Black-Box Constructions of Composable Protocols without Set-Up. CRYPTO 2012: 461-478

41. Johannes Gehrke, Michael Hay, Edward Lui, Rafael Pass: Crowd-Blending Privacy. CRYPTO 2012: 479-496

42. Mohammad Mahmoody, Rafael Pass: The Curious Case of Non-Interactive Commitments - On the Power of Black-Box vs. Non-Black-Box Use of Primitives. CRYPTO 2012: 701-718

43. Kai-Min Chung, Rafael Pass, Wei-Lung Dustin Tseng: The Knowledge Tightness of Parallel Zero-Knowledge. TCC 2012: 512-529

44. Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, Tal Rabin: Secure Computation Without Authentication. J. Cryptology 24(4): 720-760 (2011)

45. Rafael Pass, Wei-Lung Dustin Tseng, Douglas Wikstrm: On the Composition of Public-Coin Zero-Knowledge Protocols. SIAM J. Comput. 40(6): 1529-1553 (2011)

46. Joseph Y. Halpern, Rafael Pass: Algorithmic rationality: adding cost of computation to game theory. SIGecom Exchanges 10(2): 9-15 (2011)

47. Kai-Min Chung, Rafael Pass: The Randomness Complexity of Parallel Repetition. FOCS 2011: 658-667

48. Eleanor Birrell, Rafael Pass: Approximately Strategy-Proof Voting. IJCAI 2011: 67-72

49. Rafael Pass, Abhi Shelat: Renegotiation-Safe Protocols. ICS 2011: 61-78

50. Rafael Pass: Limits of provable security from standard assumptions. STOC 2011: 109-118

51. Huijia Lin, Rafael Pass: Constant-round non-malleable commitments from any one-way function. STOC 2011: 705-714

52. Adam Bjorndahl, Joseph Y. Halpern, Rafael Pass: Reasoning about justified belief. TARK 2011: 221-227

53. Huijia Lin, Rafael Pass: Concurrent Non-Malleable Zero Knowledge with Adaptive Inputs. TCC 2011: 274-292

54. Johannes Gehrke, Edward Lui, Rafael Pass: Towards Privacy for Social Networks: A Zero-Knowledge Based Definition of Privacy. TCC 2011: 432-449

55. Rafael Pass: Concurrent Security and Non-malleability. TCC 2011: 540

56. Rafael Pass, Wei-Lung Dustin Tseng, Muthuramakrishnan Venkitasubramaniam: Towards Non-Black-Box Lower Bounds in Cryptography. TCC 2011: 579-596

57. Huijia Lin, Rafael Pass, Wei-Lung Dustin Tseng, Muthuramakrishnan Venkitasubramaniam: Concurrent Non-Malleable Zero Knowledge Proofs. CRYPTO 2010: 429-446

58. Ran Canetti, Huijia Lin, Rafael Pass: Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions. FOCS 2010: 541-550

59. Joseph Y. Halpern, Rafael Pass: Game Theory with Costly Computation: Formulation and Application to Protocol Security. ICS 2010: 120-142 2010: 588-605

6 Awards and Honors during Reporting Period

- Wallenberg Academy Fellow (awarded by the Royal Academy of Science in Sweden), 2013.
- Fiona Ip Li and Donald Li Excellence in Teaching Award, 2012.
- Invited Talk at Theory of Cryptography Conference, 2011.
- Alfred P. Sloan Fellow, 2011.
- 5 paper have been selected to special issues for best papers from conferences:
  - P. Austrin, K. Chung, M. Mahmoody, R. Pass, K. Seth. *On the impossibility of Crypptography with Tamperable Randomness.* Invited to Algorithmica special issue on best papers from CRYPTO'14.
  - Rafael Pass, Huijia Lin, Muthuramakrishnan Venkitasubramaniam: *A Unified Framework for UC from Only OT.* Invited to Journal of Cryptology special issue on best paper from ASIACRYPT 2012.
  - K. Chung, R. Pass, K. Seth. *Non-black-box simulation from one-way functions and applications to resettable security.* Invited to SIAM Journal of Computing special issue on selected papers of STOC 2012.
  - R. Pass. *Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments.* Invited to Computational Complexity special issue for the ten year anniversary of TCC. Invited to Journal of Cryptology special issue on best papers from TCC 2013.
  - R. Canetti, H. Lin and R. Pass. *Adaptive Hardness and Composable Security from Standard Assumptions.* Invited to SIAM Journal of Computing special issue on selected papers of FOCS 2010.

Response ID:4683 Data

1.

1. Report Type

Final Report

Primary Contact E-mail
Contact email if there is a problem with the report.

rafael@cs.cornell.edu

Primary Contact Phone Number
Contact phone number if there is a problem with the report

6073799993

Organization / Institution name

Cornell University

Grant/Contract Title
The full title of the funded effort.

AFOSR YIP: New Models for Protocol Security

Grant/Contract Number
AFOSR assigned control number. It must begin with "FA9550" or "F49620" or "FA2386".

FA9550-10-1-0093

Principal Investigator Name
The full name of the principal investigator on the grant or contract.

Rafael Pass

Program Manager
The AFOSR Program Manager currently assigned to the award

Tristan Nguyen

Reporting Period Start Date

04/01/2010

Reporting Period End Date

03/31/2015

Abstract

Following the ground-breaking work on public-key encryption in the 70's, the field of Cryptography has evolved far beyond securing message transmission. For instance, the notion of a secure computation, introduced by Yao and Goldreich, Micali and Wigderson in the early 80's, enables a set of parties to, through the execution of a distributed communication protocol, securely implement any service that a trusted party could perform for them.

This novel use of cryptography, however, also admits new types of attacks, which require studying new models of security. During the reporting period, we have focused on two major directions within this topic: security under concurrent executions, and security under tampering attacks.

Our major results include:

* the first constant-round construction for defending

against so-called “man-in-the-middle attacks” based the minimal assumption of one-way functions; this had remained a major open problem for over 20
years.

* the first secure computation protocols that requires no trusted infrastructure other than authenticated communication, and satisfies concurrent security.

* developing new methods for dealing with security against so-called “resetting” attacks.

* initiated a study of the security of cryptographic protocols in the presence of tampering of the randomness of honest parties.

Our research has been published in the premier Computer
Science Theory conferences (STOC, FOCS, ITCS), and the premier
Cryptography conferences (CRYPTO, EuroCrypt, TCC); 5 of these papers
were selected for special issues on best papers.

Distribution Statement

This is block 12 on the SF298 form.

Distribution A - Approved for Public Release

Explanation for Distribution Statement

If this is not approved for public release, please provide a short explanation. E.g., contains proprietary information.

SF298 Form

Please attach your SF298 form. A blank SF298 can be found here. Please do not password protect or secure the PDF The maximum file size for an SF298 is 50MB.

SF298 Form_RPass AFOSR YIP.pdf

Upload the Report Document. File must be a PDF. Please do not password protect or secure the PDF . The maximum file size for the Report Document is 50MB.

final-report.pdf

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Archival Publications (published) during reporting period:

1. Huijia Lin, Rafael Pass: Constant-Round Nonmalleable Commitments from Any One-Way Function. J. ACM 62(1): 5:1-5:30 (2015)
2. Joseph Y. Halpern, Rafael Pass: Algorithmic rationality: Game theory with costly com- putation. J. Economic Theory 156: 246-268 (2015)
3. Samantha Leung, Edward Lui, Rafael Pass: Voting with Coarse Beliefs. ITCS 2015: 61
4. Jing Chen, Silvio Micali, Rafael Pass: Better Outcomes from More Rationality. ITCS 2015: 325
5. Kai-Min Chung, Edward Lui, Rafael Pass: From Weak to Strong Zero-Knowledge and Applications. TCC (1) 2015: 66-92
6. Kai-Min Chung, Rafael Pass: Tight Parallel Repetition Theorems for Public-Coin Argu- ments Using KL-Divergence. TCC (2) 2015: 229-246
7. Vipul Goyal, Huijia Lin, Omkant Pandey, Rafael Pass, Amit Sahai: Round-Efficient Con- currently Composable Secure Computation via a Robust Extraction Lemma. TCC (1) 2015: 260-289
8. Edward Lui, Rafael Pass: Outlier Privacy. TCC (2) 2015: 277-305
9. Rafael Pass, Wei-Lung Dustin Tseng, Muthuramakrishnan Venkitasubramaniam: Concur- rent Zero Knowledge, Revisited. J. Cryptology 27(1): 45-66 (2014)
10. Kai-Min Chung, Zhenming Liu, Rafael Pass: Statistically-secure ORAM with (log2 n) Overhead. ASIACRYPT (2) 2014: 62-81
11. Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, Karn Seth: On the Impossibility of Cryptography with Tamperable Randomness. CRYPTO (1) 2014: 462-479
12. Rafael Pass, Karn Seth, Sidharth Telang: Indistinguishability Obfuscation from Semantically- Secure

Multilinear Encodings. CRYPTO (1) 2014: 500-517
13. Ilan Komargodski, Tal Moran, Moni Naor, Rafael Pass, Alon Rosen, Eylon Yogev: One- Way Functions and (Im)Perfect Obfuscation. FOCS 2014: 374-383
14. Joseph Y. Halpern, Rafael Pass, Lior Seeman: The truth behind the myth of the folk theorem. ITCS 2014: 543-554
15. Adam Bjorndahl, Joseph Y. Halpern, Rafael Pass: Axiomatizing Rationality. KR 2014
16. Rafael Pass, Karn Seth: On the Impossibility of Black-Box Transformations in Mechanism Design. SAGT 2014: 279-290
17. Elette Boyle, Kai-Min Chung, Rafael Pass: On Extractability Obfuscation. TCC 2014: 52-73
18. Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Muthuramakrishnan Venkitasubramaniam, Ivan Visconti: 4-Round Resettably-Sound Zero Knowledge. TCC 2014: 192-216
19. Joseph Y. Halpern, Rafael Pass, Lior Seeman: Not Just an Empty Threat: Subgame- Perfect Equilibrium in Repeated Games Played by Computationally Bounded Players. WINE 2014: 249-262
20. Joseph Y. Halpern, Rafael Pass: Conservative belief and rationality. Games and Economic Behavior 80: 186-192 (2013)
21. Rafael Pass, Alon Rosen, Wei-Lung Dustin Tseng: Public-Coin Parallel Zero-Knowledge for NP. J. Cryptology 26(1): 1-10 (2013)
22. Kai-Min Chung, Rafael Pass: Guest column: parallel repetition theorems for interactive arguments. SIGACT News 44(1): 50-69 (2013)
23. Kai-Min Chung, Huijia Lin, Rafael Pass: Constant-Round Concurrent Zero Knowledge from P-Certificates. FOCS 2013: 50-59
24. Kai-Min Chung, Rafail Ostrovsky, Rafael Pass, Ivan Visconti: Simultaneous Resettability from One-Way Functions. FOCS 2013: 60-69
25. Ran Canetti, Huijia Lin, Rafael Pass: From Unprovability to Environmentally Friendly Protocols. FOCS 2013: 70-79
26. Kai-Min Chung, Rafael Pass, Sidharth Telang: Knowledge-Preserving Interactive Coding. FOCS 2013: 449-458
27. Adam Bjorndahl, Joseph Y. Halpern, Rafael Pass: Language-Based Games. IJCAI 2013
28. Joseph Y. Halpern, Rafael Pass: Sequential Equilibrium in Computational Games. IJCAI 2013
29. Kai-Min Chung, Edward Lui, Rafael Pass: Can theories be tested?: a cryptographic treatment of forecast testing. ITCS 2013: 47-56
30. Per Austrin, Johan Hstad, Rafael Pass: On the power of many one-bit provers. ITCS 2013: 215-220
31. Kai-Min Chung, Huijia Lin, Mohammad Mahmoody, Rafael Pass: On the power of nonuni- formity in proofs of security. ITCS 2013: 389-400
32. Kai-Min Chung, Rafael Pass, Karn Seth: Non-black-box simulation from one-way functions and applications to resettable security. STOC 2013: 231-240
33. Rafael Pass: Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments. TCC 2013: 334-354
34. Eleanor Birrell, Kai-Min Chung, Rafael Pass, Sidharth Telang: Randomness-Dependent Message Security. TCC 2013: 700-720
35. Joseph Y. Halpern, Rafael Pass: Iterated regret minimization: A new solution concept. Games and Economic Behavior 74(1): 184-207 (2012)
36. Tom Roeder, Rafael Pass, Fred B. Schneider: Multi-Verifier Signatures. J. Cryptology 25(2): 310-348 (2012)
37. Rafael Pass, Muthuramakrishnan Venkitasubramaniam: A Parallel Repetition Theorem for Constant-Round Arthur-Merlin Proofs. TOCT 4(4): 10 (2012)
38. Joseph Y. Halpern, Rafael Pass, Lior Seeman: I'm Doing as Well as I Can: Modeling People as Rational Finite Automata. AAAI 2012
39. Rafael Pass, Huijia Lin, Muthuramakrishnan Venkitasubramaniam: A Unified Framework for UC from Only OT. ASIACRYPT 2012: 699-717
40. Huijia Lin, Rafael Pass: Black-Box Constructions of Composable Protocols without Set- Up. CRYPTO 2012: 461-478
41. Johannes Gehrke, Michael Hay, Edward Lui, Rafael Pass: Crowd-Blending Privacy. CRYPTO 2012:

479-496
42. Mohammad Mahmoody, Rafael Pass: The Curious Case of Non-Interactive Commitments - On the Power of Black-Box vs. Non-Black-Box Use of Primitives. CRYPTO 2012: 701-718
43. Kai-Min Chung, Rafael Pass, Wei-Lung Dustin Tseng: The Knowledge Tightness of Par- allel Zero-Knowledge. TCC 2012: 512-529
44. Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, Tal Rabin: Secure Computation Without Authentication. J. Cryptology 24(4): 720-760 (2011)
45. Rafael Pass, Wei-Lung Dustin Tseng, Douglas Wikstrm: On the Composition of Public- Coin Zero-Knowledge Protocols. SIAM J. Comput. 40(6): 1529-1553 (2011)
46. Joseph Y. Halpern, Rafael Pass: Algorithmic rationality: adding cost of computation to game theory. SIGecom Exchanges 10(2): 9-15 (2011)
47. Kai-Min Chung, Rafael Pass: The Randomness Complexity of Parallel Repetition. FOCS 2011: 658-667
48. Eleanor Birrell, Rafael Pass: Approximately Strategy-Proof Voting. IJCAI 2011: 67-72
49. Rafael Pass, Abhi Shelat: Renegotiation-Safe Protocols. ICS 2011: 61-78
50. Rafael Pass: Limits of provable security from standard assumptions. STOC 2011: 109-118
51. Huijia Lin, Rafael Pass: Constant-round non-malleable commitments from any one-way function. STOC 2011: 705-714
52. Adam Bjorndahl, Joseph Y. Halpern, Rafael Pass: Reasoning about justified belief. TARK 2011: 221-227
53. Huijia Lin, Rafael Pass: Concurrent Non-Malleable Zero Knowledge with Adaptive Inputs. TCC 2011: 274-292
54. Johannes Gehrke, Edward Lui, Rafael Pass: Towards Privacy for Social Networks: A Zero-Knowledge Based Definition of Privacy. TCC 2011: 432-449
55. Rafael Pass: Concurrent Security and Non-malleability. TCC 2011: 540
56. Rafael Pass, Wei-Lung Dustin Tseng, Muthuramakrishnan Venkitasubramaniam: Towards Non-Black-Box Lower Bounds in Cryptography. TCC 2011: 579-596
57. Huijia Lin, Rafael Pass, Wei-Lung Dustin Tseng, Muthuramakrishnan Venkitasubrama- niam: Concurrent Non-Malleable Zero Knowledge Proofs. CRYPTO 2010: 429-446
58. Ran Canetti, Huijia Lin, Rafael Pass: Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions. FOCS 2010: 541-550
59. Joseph Y. Halpern, Rafael Pass: Game Theory with Costly Computation: Formulation and Application to Protocol Security. ICS 2010: 120-142 2010: 588-605

Changes in research objectives (if any):

Change in AFOSR Program Manager, if any:

Change from Herklotz to Tristan Nguyen

Extensions granted or milestones slipped, if any:

AFOSR LRIR Number

LRIR Title

Reporting Period

Laboratory Task Manager

Program Officer

Research Objectives

Technical Summary

Funding Summary by Cost Category (by FY, $K)

	Starting FY	FY+1	FY+2
Salary			
Equipment/Facilities			
Supplies			
Total			

Report Document

Report Document - Text Analysis

Report Document - Text Analysis

Appendix Documents

2. Thank You

E-mail user

Jun 18, 2015 17:10:34 Success: Email Sent to: rafael@cs.cornell.edu